What is claimed is:

1. A method for protection of computer memory against unauthorized access that is carried out independently of CPU, long-term storage and operating storage of the protected computer under control of an external controller provided with a native software, which method includes the following steps:

a) logging in each communication session all incoming messages into at least one external storage locked at the side of the protected computer;

b) locking the external storage input at the side of a communication link;

c) extracting from nonempty set of received messages at least one nonempty subset of files that belongs to the group of subsets consisting of:

first subset of files having standard name extensions indicating a textual or iconic nature of those files, and/or

second subset of files having standard name extensions indicating a program nature of those files, and/or

third subset of files having non-standard name extensions that can be attributed either to the first or to the second of said subsets after additional analysis; and

d) separately processing messages in each of said subsets to determine the demand in their reception and admissibility of their inclusion in data base and/or knowledge base and/or SW of the protected computer.

2. The method of claim 1 wherein each textual and/or iconic file from said first subset is displayed via a video display adapter only in the graphic mode in the shape of a pixel pattern, the demand in the received message is reviewed, and then:

in case of positive review, the pixel pattern is converted into the standard textual and/or graphic format in the active display window, and this converted file is logged directly from the active display window into the long-term storage of the protected computer, and the corresponding entry in the external storage is deleted, and

in case of negative review, the active display window is closed without storing any data, and the entry with the corresponding message in the external storage is deleted.

3. The method of claim 2 wherein said pixel pattern representing a textual and/or iconic file is formed with the usage of standard instructions for screen control.

4. The method of claim 2 or 3 wherein the video display adapter and the display are a video display adapter and a display of the protected computer.

5. The method of claim 1 wherein the standard extension in the name of each program file of said second subset is replaced with a non-standard extension, a trial run of such file is executed preferably externally of the protected computer, the demand in the message received is reviewed, and then:

in case of positive review, a received program is logged in the long-term storage of the protected computer, and the corresponding entry in the external storage is deleted, and

in case of negative review, the corresponding entry in the external storage is deleted.

6. The method of claim 1 wherein each received message of said third subset is first displayed via the video display adapter in the graphic mode only, visually identifying as a file belonging to said first subset or to said second subset, and then:

a) the demand in each identified textual and/or iconic file is reviewed by the visual analysis of the pixel pattern, and

in case of positive review, the pixel pattern is converted into a standard textual and/or graphic format in the active display window, and this converted message is directly logged from the active display window into the long-term storage of the protected computer while the corresponding entry in the external storage is deleted, and

in case of negative review, the active display window is closed without storing any data, while the corresponding entry in the external storage is deleted.

b) the standard extension in the name of each identified program file is replaced with a non-standard extension, a trial run of the program is executed preferably externally of the protected computer, the demand in the received program is reviewed, and

in case of positive review, the received program is logged in the long-term storage of the protected computer, and the corresponding entry in the external storage is deleted, and

in case of negative review, the corresponding entry in the external storage is deleted.

7. A device for protection of the computer memory against unauthorized access designed for connection between external sources of messages and at least one protected computer, comprising:

a controllable input switch,

at least one external storage adapted for logging each next set of incoming messages and temporarily storing it for the time of processing and which is connected to the external sources of messages via said controllable input switch

at least one external controller for controlling processing incoming messages provided with a permanent storage for storing a native software for processing incoming messages and having its control output connected to said external storage,

a controllable output switch, and

a framebuffer connected to a data output of said external storage adapted for converting incoming textual and/or iconic messages into graphic format and sequentially displaying the converted messages via said controllable output switch for testing and taking decision on receipt or refusal of each such message.

8. The device of claim 7 wherein said framebuffer in the mode of testing the incoming messages, is connected to said display via native framebuffer of the protected computer.

9. The device of claim 7 wherein said permanent storage is connected between said controller and said external storage.

10. The device of claim 7 which is further provided with an instruction buffer connected via input lock to at least one control output of the protected computer and then to the driving point of the controller and/or driving point of the external storage.